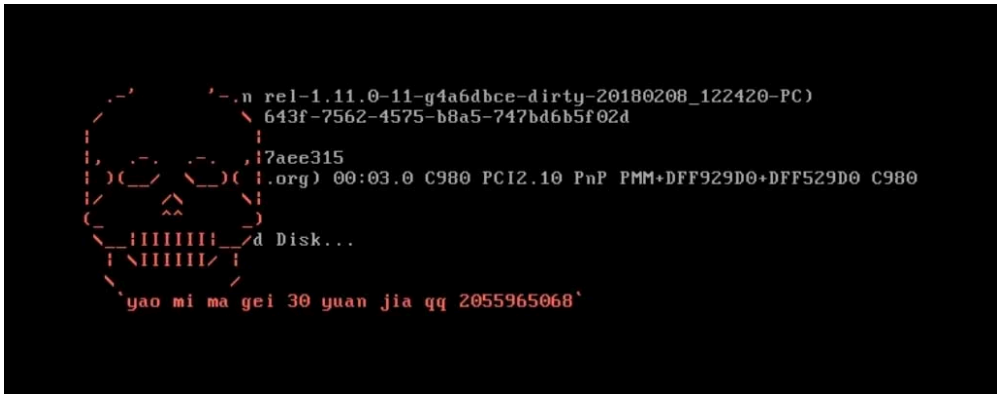
DexCrypt MBRLocker Demands 30 Yuan To Gain Access to Computer

By Lawrence Abrams

Published: 2018-02-10 · Archived: 2026-04-05 14:52:41 UTC

A new Chinese MBRLocker called DexLocker has been discovered that asks for 30 Yuan to get access to a computer. First discovered by security researcher JAMESWT, this ransomware will modify the master boot record of the victim's computer so that it shows a ransom note before Windows starts.

Unfortunately, I was not able to get this sample to run, so I have no first hand analysis of this ransomware. The AnyRun video posted by JAMESWT, though, shows that once you install the ransomware, it immediately reboots the computer and the victim is greeted with an ascii skull and a message to send 30 yaun to the 2055965068 qq address in order to get access to their computer again.

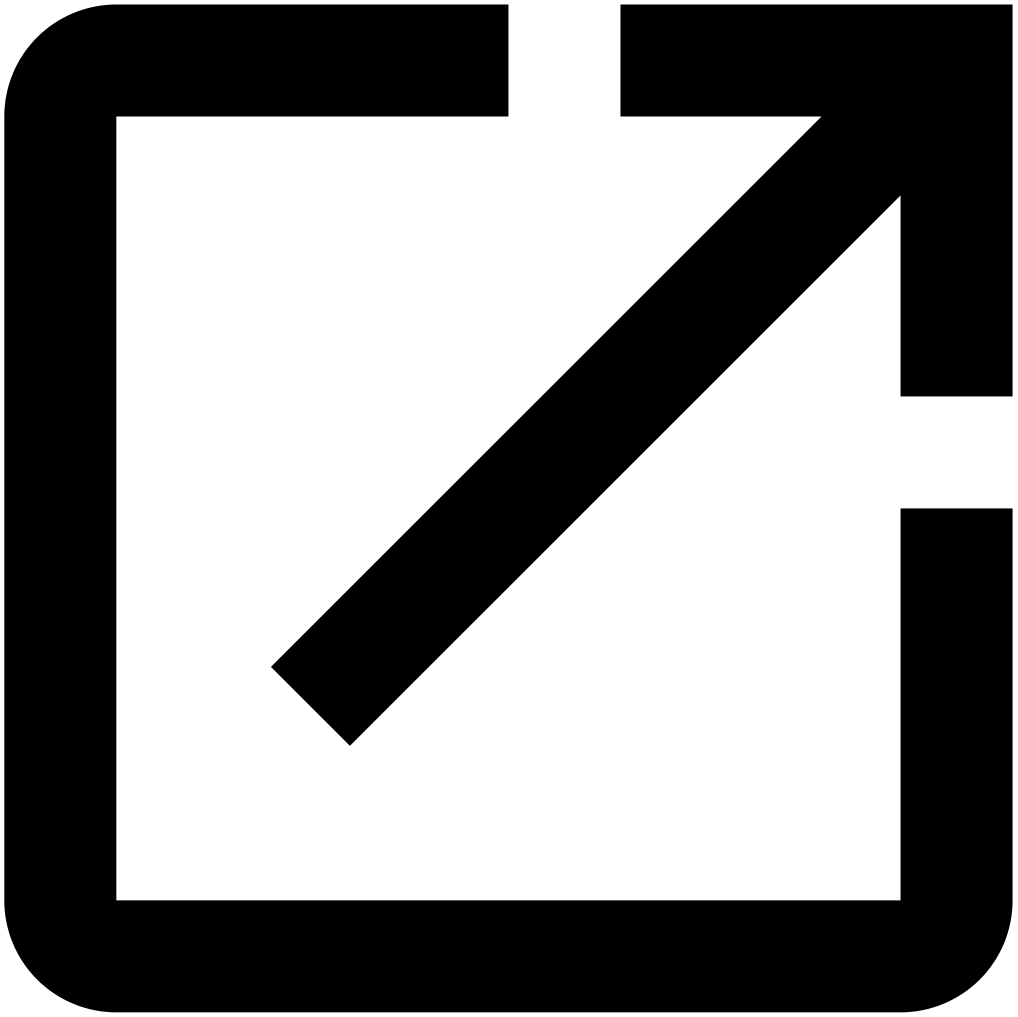


DexCrypt Lock Screen

Microsoft's Windows Defender Security Team saw Jame's tweet and tweeted that they have labeled the MBRLocker as Ransom:DOS/Dexcrypt.A and that it can be detected by Windows Defender.

According to kangxiaopao, you can enter the **ssssss** password to gain access. If this password does not work and it does only replace the MBR, it can be fixed by booting up into the Windows Recovery Console and restoring the Master Boot Record using the following commands:


DIE LINKE.
0:00



```
 bootrec /RebuildBcd
bootrec /fixMbr
bootrec /fixboot
```

Once you enter these commands, you can reboot and get access again to Windows again.

IOCs

Hashes:

```
dfc56a704b5e031f3b0d2d0ea1d06f9157758ad950483b44ac4b77d33293cb38
```

Ransom Note:

```
   .-'     '-.
 /           \
|             |
|,  .-.  .-.  ,|
| )(__/  \__)( |
|/     /\     \|
(_     ^^     _)
 \__|IIIIII|__/
  | \IIIIII/ |
  \         /
   `yao mi ma gei 30 yuan jia qq 2055965068`
```

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
